AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States of America
v.
OLUDAYO KOLAWOLE JOHN ADEAGBO
a/k/a "John Edwards" a/k/a "John Dayo"

Defendant(s)

Case No. H19-1223M

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of See offense description below in the county of Harris in the Southern District of Texas & elsewhere, the defendant(s) violated:

Code Section	*Offense Description*
	From no later than November 2016 to no earlier than July 2018, within the Southern District of Texas and elsewhere, OLUDAYO KOLAWOLE JOHN ADEAGBO a/k/a "John Edwards" a/k/a "John Dayo," did knowingly combine, conspire, confederate and agree with others known and unknown to the Grand Jury, to commit the offense of wire fraud against the United States, in violation of 18 USC 1349, as well as to commit the offense of wire fraud, in violation of 18 USC 1343.

This criminal complaint is based on these facts:

See attached affidavit.

☑ Continued on the attached sheet.

Complainant's signature

HONG NGUYEN, JR. - FBI SPECIAL AGENT
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/18/19

Judge's signature

City and state: Houston, Texas

Magistrate Judge Peter Bray
Printed name and title

AFFIDAVIT

I, Special Agent Hong Nguyen, Jr., being first duly sworn, hereby depose and state as follows:

Summary

The Federal Bureau of Investigation ("FBI") is investigating a business email compromise ("BEC") scheme that targets universities, school districts, municipalities, construction companies, and corporations. The conspirators pose as business partners (such as suppliers) of these victims, and send fraudulent emails, saying that the "supplier" has changed banks, and asks that payments be sent to a new bank account that is controlled by the conspirators. The victims think they are paying their suppliers, but in reality, their suppliers are unaware that these emails are being sent. When the victims send the money, the conspirators withdraw the money as soon as it becomes available – and before the victim can realize its mistake and cancel the transaction. The conspirators continue to be engaged in this and similar frauds as recently as May of 2018.

The FBI submits there is probable cause to believe that OLUDAYO KOLAWOLE JOHN ADEAGBO a/k/a "John Edwards" a/k/a "John Dayo" ("ADEAGBO") is conspiring with others to facilitate a multi-million dollar BEC scheme. Thus, the FBI seeks a warrant to arrest ADEAGBO.

Introduction and Agent Background

1. Affiant makes this affidavit in support of a criminal complaint and arrest warrant for ADEAGBO for violations of 18 U.S.C. §§ 1343 (wire fraud) and 1349 (conspiracy to commit wire fraud) (collectively, the Subject Offenses).

2. Affiant is a Special Agent with the FBI, and assigned to a Cyber Task Force in the Houston, Texas division. Affiant has been a Special Agent with the FBI since May 2016. As a Special Agent of the FBI, Affiant is charged with the duty of investigating violations of the laws

of the United States, collecting evidence in cases in which the United States is or may be a party in interest, and performing other duties imposed by law. Affiant investigates crimes involving the unauthorized intrusion into a computer or network such as computer intrusions, business email compromises, distributed denial-of-service attacks, ransomware, and financially motivated attacks.

3. Prior to this assignment, Affiant was a Digital Forensic Examiner at the Houston Regional Computer Forensics Laboratory where Affiant worked a variety of matters, many of which included a significant cyber component. Affiant has training in the preparation, presentation, and service of criminal arrest and search warrants. Affiant has been involved in the investigation of offenses against the United States, including fraud and related activity in connection with computers.

4. The facts set forth in this affidavit are based upon Affiant's own personal observations, training and experience, as well as information obtained during this investigation from other sources, including: (a) other agents from the FBI, and other law enforcement personnel involved in this investigation; (b) statements made or reported by various witnesses with personal knowledge of relevant facts; and (c) Affiant's review of records obtained during the course of this investigation, as well as summaries and analyses of such documents and records that have been prepared by others.

Facts Supporting Probable Cause

BEC of Victim Company A and B

5. Affiant learned that Victim Company A ("Victim A"), located in the Southern District of Texas, is a government county in the U.S. state of Texas. Victim A informed Affiant that an unauthorized person(s) impersonating (spoofed) an employee of Victim Company B

("Victim B"), sent emails from accounts@lucasconstruct.com. On or about March 13, 2018, the email stated, "Please find attached our completed ACH form and a copy of a voided check as requested. Kindly let us know once updated."

6. Victim B is a family owned construction company based in League City, Texas. Based on my training and experience, an automatic clearing house ("ACH") is a network that coordinates electronic payments and automated money transfers. Based on my training and experience, an ACH form is a document companies provide to customers and vendors to update their routing and bank account number to initiate payment for invoiced services. The ACH form attached to the email listed a SunTrust bank account ending in 6134.

7. On or about May 22, 2018, Victim A wired approximately $525,282.39 via ACH to the SunTrust bank account ending in 6134. Victim A thought the payment was for a legitimate business transaction for services they had requested. However, Affiant learned that Victim B never authorized the email requesting updated payment information to Victim A.

8. Affiant obtained information from Victim A that the domain used in the fraudulent email, lucasconstruct.com, was not the actual domain of Victim B, but a "spoofed" one (that is, a false one). Based on my training and experience, email spoofing is a fraudulent email activity that hides an email's actual origins. Affiant knows from training and experience that a domain is an organization's unique name on the Internet. The domain name server ("DNS") is what translates the domain name to an IP address. A spoofed domain is the unauthorized use of a third-party domain name in an email message in order to pretend to be someone else.

9. Affiant conducted a domain lookup on lucasconstruct.com and discovered that the spoofed domain was registered via Namecheap, Inc. ("Namecheap"), a domain registration service.

BEC of Victim Company C and D

10. Affiant learned that Victim Company C ("Victim C"), located in the Southern District of Texas, is a community college in the Greater Houston, Texas area and was targeted through an attempted BEC scheme for approximately $1,995,168.64. Victim C informed Affiant that an unauthorized person(s) impersonating (spoofed) an employee of Victim Company D ("Victim D"), sent emails from accounts@tellepsengroup.com.

11. Victim D is a family owned commercial, industrial, and concrete construction company headquartered in Houston, Texas. Victim C was instructed to send an ACH to a PNC Bank account number ending in 1887.

12. On or about March 23, 2018, Victim C wired approximately $1,995,168.64 via ACH to the PNC Bank account ending in 1887. Victim C thought the payment was for a legitimate business transaction for services they had requested. Affiant learned that Victim D never authorized the email requesting updated payment information to Victim C.

13. Affiant learned that the domain, tellepsengroup.com, was not the actual domain of Company D, but a spoofed one. Affiant conducted a domain lookup on tellepsengroup.com and discovered that, as above, the spoofed domain was registered via Namecheap.

BEC of Victim Company E and F

14. Affiant learned that Victim Company E ("Victim E"), located in the Southern District of Texas, is a government county in the U.S. state of Texas and was targeted through an attempted BEC scheme for approximately $888,009.40. Affiant learned from Victim E that an unauthorized person(s) impersonating (spoofed) an employee of Victim Company F ("Victim F"), sent emails from accounts@dwcontractorsgroup.com.

15. Victim F is a general contractor located in the Southern District of Texas. Victim E was instructed to send an ACH to a JP Morgan Chase ("Chase") account ending in 6002.

16. On or about October 12, 2017, Victim E wired two payments of $880,089.40 and $7,920.00, totaling $888,009.40 via ACH to the Chase bank account ending in 6002. Victim E thought the payment was for a legitimate business transaction for services they had requested.

17. Affiant learned that Victim F never authorized the email requesting updated payment information to Victim E.

18. Affiant learned that the domain, dwcontractorsgroup.com, was not the actual domain of Company F, but a spoofed one. Affiant conducted a domain lookup on dwcontractorsgroup.com and discovered that the spoofed domain was again registered via Namecheap.

Namecheap records lead to danielroberts604, danielroberts605, and danielroberts606

19. Affiant obtained records from Namecheap. These records indicated that the domain lucasconstruct.com was registered by someone who used the username danielroberts604 and email danielroberts604@mail.com.

20. Affiant learned that pursuant to another Court Order, NameCheap provided documents to the FBI that identified all accounts that used owner name "Daniel Roberts." Similarly, Namecheap records listed "Daniel Roberts" as owning the following accounts:

- Account #1: danielroberts604 with email as: danielroberts604@mail.com
- Account #2: danielroberts605 with email as: danielroberts605@mail.com
- Account #3: danielroberts606 with email as: danielroberts606@mail.com

21. Affiant examined the documents Namecheap provided for accounts associated with usernames danielroberts604, danielroberts605, and danielroberts606. Affiant found that all three

Daniel Roberts accounts registered a large number of domain names that were associated with construction companies. For example, danielroberts604 registered the following:

a. Tellepsengroup.com on March 19, 2018

b. D1construct.com on May 15, 2018

c. Southwoodbuilding.com on June 12, 2018

The domains are very similar to – but different from – the actual domains that are used by legitimate companies: tellepsen.com, d1construction.com, and southwoodbuilders.com.

22. Affiant noticed that all three accounts registered many other domain names that were associated with construction companies. The FBI later discovered that some of these domains were used to target additional victims in the Southern District of Texas.

1&1 Media email account records are linked to "John Edwards," an alias of ADEAGBO

23. The FBI obtained records for danielroberts604@mail.com, danielroberts605@mail.com, and danielroberts606@mail.com from the provider, 1&1 Mail and Media, Inc ("1&1 Mail").

24. In the emails obtained from danielroberts604@mail.com Affiant identified an airline ticket reservation forwarded on August 24, 2016 from oade@mail.com. The reservation was for OLUDAYO ADEAGBO.

25. In addition, Affiant observed in danielroberts604@mail.com emails that reflect status updates of possible BEC victims and domains used to defraud other companies. For example, Affiant observed in email account danielroberts604@mail.com an email with the subject line Accounts ISD Bk up. In the body of the email, Affiant observed the domain rodgersbuildersinc.com in the email, which was used to BEC Company G, a known victim tied to FBI Charlotte's investigation. Affiant also identified the domain

leelewisusa.com, which was used to BEC victim Company H, an independent school district in the Greater Dallas, Texas area.

DanielRoberts604@mail.com also contained other emails that are consistent with BEC frauds

26. Affiant also noticed that in the email with subject line Accounts ISD Bk up, the body of the email contained bank account information to include an account associated with co-conspirator 2 ("CC2"). Affiant believes that the co-conspirators most likely intended these bank accounts to serve as the beneficiary accounts for payment from the victim companies. Affiant noticed that the subjects included numerous notes in these emails. Affiant believes that the co-conspirators likely used this information to help manage their numerous schemes.

27. Affiant found that the co-conspirators used the danielroberts604@mail.com account extensively to facilitate the execution of the scheme outlined previously. For example, Affiant found numerous emails that contained the company names and contact information for the companies that owned the contracts awarded. Co-conspirators typically included the company names, addresses, contact information, and the name of the project manager for the companies awarded the contracts. Affiant observed that the links in the emails redirected to a website hosted by CMDGroup ("CMD") which contained project details.

28. Affiant noticed that an email had the subject line CMD Follow up – Construction and listed the account name ROBERTS & CO. in the body. Affiant believes that CMD refers to Construction Market Data, a ConstructConnect company, which holds itself out as a leading construction information business, provides accurate and reliable project leads to find work faster and easier. According to CMD, it tracks hundreds of thousands of commercial and civil projects throughout the U.S. and Canada to help identify business opportunities. Affiant believes based on

the investigation and records that the conspirators used CMD to search for construction projects in order to target their BEC victims.

The person who accessed this CMD account listed JohnEdwards79@yahoo.co.uk as a means of contact

29. To identify the person who was accessing these CMD records via the ROBERTS & CO. account, the FBI obtained records from CMD. These records listed the contact information as: account number A00038098, account owner John Edwards, addresses 1270 Hasen Hurst Drive, Apt. 12, West Hollywood, CA 90046 and 14 College Gardens, London, GB E47ALG. Similarly, CMD records showed that the name on the credit card used to pay CMD was "John Edwards." Notably, the person who accessed this CMD account listed JohnEdwards79@yahoo.co.uk as his email address.

30. Affiant observed that the telephone number listed as a point of contact was 447-973-3594. This telephone number is similar to that associated with ADEAGBO, 44 7973359482. Affiant learned from the records provided by CMD that the user of the account queried several construction projects located in the Southern District of Texas.

JohnEdwards79@yahoo.co.uk and "John Edwards" appear to be aliases of OLUDAYO "John" ADEAGBO

31. To learn about the person using JohnEdwards79@yahoo.co.uk, the FBI obtained records from Yahoo. According to these records, the user who opened the account listed his information as Mr john edwards, address 1 Elm tree court, City London, Country United Kingdom, zip/postal code se77dp, birthday April 6, 1979, phone number 44 7973359482. The verified alternate email was JohnDayoA@msn.com.

32. An email in JohnEdwards79@yahoo.co.uk contained a scan of a UK driver's license for JOHN EDWARDS with the following identifiers: 1. EDWARDS, 2. JOHN, 3. 06.04.1979 NIGERIA, 4a. 25.09.2015, 4b. 24.09.2025, 4c. DVLA, 5. EDWAR704069J99LK 45, 7. A signature appears here 8. COLLEGE GARDENS, LONDON, E4 7LG, 9. AM/A/B1/B/f/k/l/n/p/q.

33. OludayoAdeagbo@yahoo.co.uk appears to be an alias of JohnEdwards79@yahoo.co.uk. When the FBI obtained emails associated JohnEdwards79@yahoo.co.uk, Yahoo also produced emails that appear to be from OludayoAdeagbo@yahoo.co.uk. One possibility is that OludayoAdeagbo@yahoo.co.uk is an alias where emails sent to this address are received by JohnEdwards79@yahoo.co.uk. Based on my training and experience, an alias allows a user the benefit of having two email addresses while still accessing received emails from one convenient location. The user can use the same password and have one combined inbox for both accounts. Regardless, Affiant found two scans of Nigerian passports with the following identifiers:

	Passport #1	Passport #2
Type:	P	P
Country Code:	NGA	NGA
Passport No.	A1368588	A06774353
Surname:	ADEAGBO	ADEAGBO
Given name:	OLUDAYO KOLAWOLE JOHN	OLUDAYO KOLAWOLE JOHN
Nationality:	Nigerian	Nigerian
Date of birth:	06 APR / AVR 79	06 APR / AVR 79
Sex:	M	M
Place of birth:	Ibadan	Ibadan
Authority:	477	London UK
Date of Issue:	30 JUN / JUIN 03	17 AUG / AOU 15
Date of Expiry:	29 JUN / JUIN 08	16 AUG / AOU 20

The names on these passports, Oludayo John Kolawole Adeagbo, is consistent with JohnDayoA@msn.com, the verified alternate email address that the user provided when he created JohnEdwards79@yahoo.co.uk.

34. Affiant also found a scan of a UK passport with the following identifiers:

	Passport #3
Type:	P
Country Code:	GBR
Passport No.	093120143
Surname:	EDWARDS
Given name:	JOHN
Nationality:	British Citizen
Date of birth:	06 APR / AVR 79
Sex:	M
Place of birth:	Nigeria
Authority:	UKPA
Date of Issue:	12 JUL / JUI 04
Date of Expiry:	12 JUL / JUI 14

35. Affiant believes that Oludayo Kolawole John Adeagbo is using the alias "John Edwards." Affiant compared the photos of the Nigerian passport of ADEAGBO and the UK driver's license and UK passport of "John Edwards" and the photos appear to be the same individual, ADEAGBO. In addition, both the UK driver's license, UK passport, and Nigerian passport listed the same date of birth of April 6, 1979.

ADEAGBO was previously arrested in the UK

36. Affiant conducted open source research on ADEAGBO and found an article from BBC News titled "iPod car theft ringleader jailed." The article stated that ADEAGBO was from Charlton, south-east London, whose gang "hijacked" identities to drive off Jaguars, Mercedes, BMW's and a Porsche, before selling them on. ADEAGBO admitted conspiring to defraud between December 2001 and October 2002.

The person who accessed DanielRoberts604@mail.com on Jan. 24, 2019 also accessed his Apple account for JohnEdwards79@yahoo.co.uk on that same date

37. JohnEdwards79@yahoo.co.uk also contained an email from Apple. Records obtained from Apple for the Apple account linked to JohnEdwards79@yahoo.co.uk show that the user accessed that Apple account on Jan. 24, 2019 around 00:03:32 UTC from IP address 86.149.86.161.

38. That same day, around 06:47:44, the user of danielroberts604@mail.com accessed that account from the same IP address:

IP address: 86.149.86.161, Date: 2019-01-24 06:47:44 - (1&1 Media)

Thus, this helps corroborate that the same person who used danielroberts604@mail.com also used JohnEdwards79@yahoo.co.uk.

The same person who accessed danielroberts604's Namecheap account also accessed JohnEdwards79@yahoo.co.uk's LocalBitcoins account.

39. JohnEdwards79@yahoo.co.uk also contained an email from LocalBitcoins.com. Based on my training and experience, LocalBitcoins is a person-to-person bitcoin trading site. Records obtained from LocalBitcoins show that on February 28, 2018, IP address 81.153.182.196, attempted to access johnedwards79's LocalBitcoins account. danielroberts604's Namecheap account was also accessed on the same date and from the same IP address (81.153.182.196).

- IP address: 81.153.182.196, Date: 2018-02-28 2:13:52 PM (Namecheap)
- IP address: 81.153.182.196, Date: 2018-02-28 16:19 - UTC (LocalBitcoins)

OludayoAdeagbo@yahoo.co.uk contained statements for Santander Bank accounts -4924 and -7282 in the name of ADEAGBO

40. Among the emails that Yahoo produced for OludayoAdeagbo@yahoo.co.uk included email notifications from Santander Bank regarding accounts ended in 4924 and 7282 in the name of OLUDAYO KOLAWOLE ADEAGBO.

Records for the Coinbase account linked to JohnEdwards79@yahoo.co.uk show photos of what appears to be ADEAGBO, as well as references to his address at 12 College Gardens

41. JohnEdwards79@yahoo.co.uk also contained emails from Coinbase. In turn, the FBI requested records from Coinbase regarding the Coinbase account linked to JohnEdwards79@yahoo.co.uk. In response, Coinbase produced the following:

Name: JOHN EDWARDS
Email: johnedwards79@yahoo.co.uk
Date of birth 4/6/1979
Street address 12 College Gardens,
London, GB E4 7LG
Phone: 7973359482
Verified driver's license
EDWAR704069J99LK45
User ID: 59fb993bcc4b7f00bf412211

Name: DONALD ECHEAZU
Email: diecheazu@yahoo.co.uk
Phone: 7837887959
User ID: 5a395cac338e91021b1856f3

42. Coinbase also provided three photos associated with this account. The first photo was the same UK driver's license for "John Edwards" found in JohnEdwards79@yahoo.co.uk with the same driver's license number. The second photo was a self-portrait of an individual whose picture is consistent with ADEAGBO aka "John Edwards." The third photo was the UK passport for ECHEAZU, which appears to be the same passport found in DIEcheazu@yahoo.co.uk, a suspected co-conspirator.

43. Similarly, the Coinbase account listed three payment cards with the following identifiers:

	Card with last four digits 1713	Card with last four digits 0312	Card with last four digits 4419
Name	John Edwards	J Edwards	John Edwards
Expiration	01/2019	11/2020	04/2020
Type	Visa debit	Visa debit	Visa debit
Issuer	TSB Bank PLC	TSB Bank PLC	HSBC Bank PLC
Address	12 College Gardens, Chingford, London, GB E47LG	12 College Gardens, Chingford, London, GB E47LG	12 College Gardens, Chingford, London, GB E47LG

"John Dayo" and Co-Conspirator #1 ("CC1") communicate about accounts via WhatsApp messages

44. Affiant learned that on or about April 17, 2017, pursuant to U.S. Homeland Security Investigations/Customs Border Protection authority ("HSI/CBP") at the Los Angeles International Airport ("LAX"), HSI/CBP conducted a border search on CC1 as he entered the country from London, U.K. HSI/CBP provided the results to the FBI Charlotte and subsequently to the FBI Houston for additional analysis.

42. According to the phone dump, CC1 chatted with someone using the screen name John Dayo, using WhatsApp, a messaging service, to discuss bank accounts, business, and distribution of funds to name a few. John Dayo's listed phone number for the WhatsApp chats is 447973359482, which is the same U.K. number for ADEAGBO.

43. Affiant observed the following conversation:

November 07, 2016

> John Dayo: When is [FBI redacted due to containing nickname for CC2] calling that bank
>
> CC1: The guy gets on my nerves regarding this all business
>
> CC1: He sent me a screen grab of the acc which I told him to forward to you but I have now done that

John Dayo: Ok

John Dayo: He said he wanted to call that palga

[…]

November 15, 2016

CC1: J E has one for the secondary that he said he would send last night or this morning, I didn't get it last night so I'm expecting it this morning

John Dayo: Cool

John Dayo: Need a logo bro

John Dayo: For [name redacted as FBI believes this was a BEC victim]

CC1: You know I've got you

[…]

November 22, 2016

[…]

John Dayo: Get the guy to open up a chase for his business

November 28, 2016

John Dayo: What's happening with this buddy pass

November 29, 2016

[…]

John Dayo: You need to stop insulting him because it's business, you need to be insisting on meeting him.

CC1: I had planned with what was supposed to happen yesterday and it didn't happen I called him to over 20 times and this the only he responds

John Dayo: We shouldn't have done his account

John Dayo: Your guys confirmed

CC1: Not yet J

John Dayo: Let me know when they do

CC1: Yes I will

December 03, 2016

[…]

John Dayo: The 12m never land yet

CC1: The guy is out but will send the screenshot once he gets home

CC1: There just $8 in there

John Dayo: The account isn't showing on the telephone banking anymore

John Dayo: Get a screenshot

December 09, 2016

John Dayo: [FBI believes this was a BEC victim and therefore redacted the organization name]

December 11, 2016

John Dayo: Please I need these business cards

"John Dayo" provided JohnEdwards79@yahoo.co.uk as his email address and thus, appears to be OLUDAYO "John" ADEAGBO

December 13, 2016

CC1: It me [FBI redacted due to containing CC1 first name]

John Dayo: Johnedwards79@yahoo.co.uk
morayo01

CC1: Nothing is getting sent out today from the 1.9, but they will send something tomorrow I am just waiting to confirm the amount and to make sure that it happens firs thing that is what [FBI redacted due to containing CC2 identifier] told me.

CC1: I have asked to see if they can get something out today and [CC2] is adamant that nothing is going out. But once he confirms with [FBI redacted containing

potential co-conspirator's 3 name ("CC3")] on what's is going out tomorrow he will pass on the info to yourself.

CC1: I will chase them to make if first thing in the am.

John Dayo: cool.

December 14, 2016

CC1: It's so frustrating having no control over how much gets sent, with [CC2] his telling me that they questioned the ac holder for 3hrs (I don't understand why and why they didn't send anything from the 4m today either). [CC2] said that they sent just over 260$ late so will have to see if its shows up in secondary tomorrow fingers crossed.

CC1: The procedures are too slow

December 15, 2016

John Dayo: No problem, there's no rush in the 4m.

"John Dayo" sends a screenshot of a Bank of America account which contains the name "OLUDAYO KOLAWOLE JOHN ADEAGBO"

January 04, 2017

CC1: Big J can you send me you act info again Please

John Dayo: [Sent a screenshot of a Bank of America account number 325080601285, under the name OLUDAYO KOLAWOLE JOHN ADEAGBO, with address 1270 Havenhurst Dr Apt, 12, West Hollywood, United Kingdom]

CC1: Thanks

John Dayo: Cool Mitch

[…]

CC1: Check your acc mate

John Dayo: What's in my account

John Dayo: 1,775

CC1: Yup

[…]

CC1: I pray for the day that I can send you money for the heck of it, in the not too far future with many zeros will follow that

John Dayo: Amen

CC1: Tola 200quid

John Dayo: It's about 1400

CC1: Xavion's mum 1,250

John Dayo: It's not 1500 you mitch

John Dayo: Do ur math

CC1: When I checked xe it was that but I will send the rest now

[…]

January 15, 2017

John Dayo: Yo [CC1]

CC1: What's good family

John Dayo: What's happening with the buddy pass?

John Dayo: Tell [CC2] I want my money back

[…]

CC1: Yeah I told him and we are getting our money back

[…]

Pictures that "John Dayo" sent are consistent with ADEAGBO's Nigerian passports – and with "John Edwards'" U.K. driver's license and passport

64. Affiant learned from the WhatsApp conversations that on or about February 10, 2017, John Dayo sent CC1 a photo depicting his face and upper body. Affiant reviewed the photo

of John Dayo and it matched the face of the U.K. driver's license and passport of John Edwards, and the two Nigerian Passports of ADEAGBO.

65. On or about April 16, 2017, CC1 sent a photo to John Dayo depicting a photo of two individuals in a black sports car. Affiant reviewed the photo and the driver of the black vehicle matches the description of ADEAGBO a/k/a "John Edwards".

66. Affiant reviewed the photo of the vehicle and it appeared to be a black Porsche. This is consistent with parking ticket from London Borough of Lambeth found in email account JohnEdwards79@yahoo.co.uk. The email discusses a parking challenge submitted by "John Edwards" of 12 College Gardens, London, Greater London, E4 7LG for a black Porsche (vehicle registration mark D10APT).

67. Affiant conducted open source research and found that the username John Dayo is associated with a Facebook account. Affiant reviewed John Dayo's profile photos and the photos depicted the same person as ADEAGBO a/k/a John Edwards.

68. Affiant conducted open source research on telephone number 44 7973359482 and found accounts tied to ADEAGBO's Facebook, Whatsapp, Viber, Telegram accounts. This number was also in the subscriber information for email account JohnEdwards79@yahoo.co.uk.

Previously, ADEAGBO used his Bank of America account to pay for CMD

69. The FBI requested records for Bank of America ("BOA") account numbers ending in 1285 and 1298. The FBI identified these accounts from the Whatsapp chats with CC1. The name on the signature card is OLUDAYO KOLAWOLE JOHN ADEAGBO, passport# A06774353, address 1270 Hasen Hurst Drive, Apt. 12, West Hollywood, CA 90046. Both BOA accounts were opened on August 31, 2016.

70. These records showed two transactions to CMD, provider of business information for the North American construction industry as stated above, totaling $4,510 from BOA account ending in 1285. One payment was for $2,835 on September 28, 2016 and another was for $1,675 on October 12, 2016.

TECHNICAL TERMS

79. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. "Records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

80. For these reasons, I ask the Court to authorize this warrant.

Hong Nguyen, Jr.
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 18, 2019.

I find probable cause to authorize this warrant.

U.S. Magistrate Judge Peter Bray